Detecting and Preventing Cyber Insider Threats: A Surv

IEEE Communications Surveys and Tutorials

20, 1397-1417

DOI: 10.1109/comst.2018.2800740

Citation Report

#	Article	IF	Citations
1	An Approach to Enhancing Confidentiality and Integrity on Mobile Multi-Cloud Systems: The â€œARIANNAâ€• Experience. , 2018, , .		1
2	Anomaly-Based Insider Threat Detection Using Deep Autoencoders. , 2018, , .		40
3	Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations. , 2018, , .		4
4	An Algorithm for Generating Invisible Data Poisoning Using Adversarial Noise That Breaks Image Classification Deep Learning. Machine Learning and Knowledge Extraction, 2018, 1, 192-204.	3.2	7
5	An Indirect-Direct event-triggered mechanism for networked control system against DoS attacks. , 2018, , .		1
6	Getting Prepared for the Next Botnet Attack : Detecting Algorithmically Generated Domains in Botnet Command and Control. , 2018, , .		9
7	Moving Target Defense Against Advanced Persistent Threats for Cybersecurity Enhancement. , 2018, , .		5
8	The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. Computer Law and Security Review, 2018, 34, 1180-1196.	1.3	26
9	E-AUA: An Efficient Anonymous User Authentication Protocol for Mobile IoT. IEEE Internet of Things Journal, 2019, 6, 1506-1519.	5.5	80
10	Predicting day-ahead solar irradiance through gated recurrent unit using weather forecasting data. Journal of Renewable and Sustainable Energy, 2019, 11, .	0.8	36
11	How Much Enhancing Confidentiality and Integrity on Data Can Affect Mobile Multi-Cloud: The "ARIANNA" Experience. , 2019, , .		1
12	Augmented-reality-driven medical simulation platform for percutaneous nephrolithotomy with cybersecurity awareness. International Journal of Distributed Sensor Networks, 2019, 15, 155014771984017.	1.3	9
13	A Trust Aware Unsupervised Learning Approach for Insider Threat Detection. , 2019, , .		15
14	On Dynamic Recovery of Cloud Storage System Under Advanced Persistent Threats. IEEE Access, 2019, 7, 103556-103569.	2.6	12
15	Changes in Binocular Color Fusion Limit Caused by Different Disparities. IEEE Access, 2019, 7, 70088-70101.	2.6	5
16	A Secure Fine-Grained Micro-Video Subscribing System in Cloud Computing. IEEE Access, 2019, 7, 137266-137278.	2.6	2
17	A3CM: Automatic Capability Annotation for Android Malware. IEEE Access, 2019, 7, 147156-147168.	2.6	29
18	Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System. IEEE Internet of Things Journal, 2019, 6, 9794-9805.	5.5	62

#	Article	IF	Citations
19	Privacy-preserving big data analytics a comprehensive survey. Journal of Parallel and Distributed Computing, 2019, 134, 207-218.	2.7	58
20	A Lightweight Assisted Vulnerability Discovery Method Using Deep Neural Networks. IEEE Access, 2019, 7, 80079-80092.	2.6	18
21	A reversible sketch-based method for detecting and mitigating amplification attacks. Journal of Network and Computer Applications, 2019, 142, 15-24.	5.8	23
22	Employee profiling via aspect-based sentiment and network for insider threats detection. Expert Systems With Applications, 2019, 135, 351-361.	4.4	29
23	Predicting the Impact of Android Malicious Samples via Machine Learning. IEEE Access, 2019, 7, 66304-66316.	2.6	16
24	An innovative approach for real-time network traffic classification. Computer Networks, 2019, 158, 143-157.	3.2	76
25	Static malware clustering using enhanced deep embedding method. Concurrency Computation Practice and Experience, 2019, 31, e5234.	1.4	11
26	An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning. Security and Communication Networks, 2019, 2019, 1-12.	1.0	41
27	Editorial: Recent advances in machine learning for cybersecurity. Concurrency Computation Practice and Experience, 2019, 31, e5270.	1.4	0
28	Machine learningâ€"based hapticâ€enabled surgical navigation with security awareness. Concurrency Computation Practice and Experience, 2019, 31, e4908.	1.4	1
29	PGSM-DPI: Precisely Guided Signature Matching of Deep Packet Inspection for Traffic Analysis. , 2019, , .		2
30	Information Security Insider Threats in Organizations and Mitigation Techniques. , 2019, , .		3
31	Insider Threat Detection via Hierarchical Neural Temporal Point Processes. , 2019, , .		18
32	Exploring Feature Normalization and Temporal Information for Machine Learning Based Insider Threat Detection. , 2019, , .		28
33	Insider Threat Identification Using the Simultaneous Neural Learning of Multi-Source Logs. IEEE Access, 2019, 7, 183162-183176.	2.6	22
34	Dynamic Insider Threat Detection Based on Adaptable Genetic Programming. , 2019, , .		4
35	Embedding Learning with Heterogeneous Event Sequence for Insider Threat Detection. , 2019, , .		3
36	Detecting IRC-based Botnets by Network Traffic Analysis Through Machine Learning. , 2019, , .		1

#	Article	IF	Citations
37	Comparison of Nikto and Uniscan for measuring URL vulnerability. , 2019, , .		3
38	DeepBalance: Deep-Learning and Fuzzy Oversampling for Vulnerability Detection. IEEE Transactions on Fuzzy Systems, 2019, , 1-1.	6.5	50
39	Î¼VulDeePecker: A Deep Learning-Based System for Multiclass Vulnerability Detection. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	65
40	An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT. IEEE Access, 2019, 7, 180205-180217.	2.6	27
41	Intranet User-Level Security Traffic Management with Deep Reinforcement Learning. , 2019, , .		3
42	GUI-Squatting Attack: Automated Generation of Android Phishing Apps. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	20
43	A performance evaluation of deepâ€learnt features for software vulnerability detection. Concurrency Computation Practice and Experience, 2019, 31, e5103.	1.4	28
44	Design of multi-view based email classification for IoT systems via semi-supervised learning. Journal of Network and Computer Applications, 2019, 128, 56-63.	5.8	40
45	Multidimensional privacy preservation in location-based services. Future Generation Computer Systems, 2019, 93, 312-326.	4.9	31
46	Data-Driven Cybersecurity Incident Prediction: A Survey. IEEE Communications Surveys and Tutorials, 2019, 21, 1744-1772.	24.8	216
47	Efficient cloud-aided verifiable secret sharing scheme with batch verification for smart cities. Future Generation Computer Systems, 2020, 109, 450-456.	4.9	11
48	Distributed Event-Triggered Estimation Over Sensor Networks: A Survey. IEEE Transactions on Cybernetics, 2020, 50, 1306-1320.	6.2	322
49	Secure real-time image protection scheme with near-duplicate detection in cloud computing. Journal of Real-Time Image Processing, 2020, 17, 175-184.	2.2	12
50	Distributed Cyber Attacks Detection and Recovery Mechanism for Vehicle Platooning. IEEE Transactions on Intelligent Transportation Systems, 2020, 21, 3821-3834.	4.7	91
51	Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC. IEEE Systems Journal, 2020, 14, 1972-1983.	2.9	16
52	VASABI: Hierarchical User Profiles for Interactive Visual User Behaviour Analytics. IEEE Transactions on Visualization and Computer Graphics, 2020, 26, 77-86.	2.9	24
53	Model-based evaluation of combinations of Shuffle and Diversity MTD techniques on the cloud. Future Generation Computer Systems, 2020, 111, 507-522.	4.9	14
54	Data-Driven Cyber Security in Perspectiveâ€”Intelligent Traffic Analysis. IEEE Transactions on Cybernetics, 2020, 50, 3081-3093.	6.2	78

#	Article	IF	Citations
55	Effective Quarantine and Recovery Scheme Against Advanced Persistent Threat. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51, 5977-5991.	5.9	17
56	Load Distributed and Benign-Bot Mitigation Methods for IoT DNS Flood Attacks. IEEE Internet of Things Journal, 2020, 7, 986-1000.	5.5	18
57	Cyber Vulnerability Intelligence for Internet of Things Binary. IEEE Transactions on Industrial Informatics, 2020, 16, 2154-2163.	7.2	34
58	Software Vulnerability Discovery via Learning Multi-Domain Knowledge Bases. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 2469-2485.	3.7	52
59	Neural Model Stealing Attack to Smart Mobile Device on Intelligent Medical Platform. Wireless Communications and Mobile Computing, 2020, 2020, 1-10.	0.8	4
60	Performance-based Comparative Analysis of Open Source Vulnerability Testing Tools for Web Database Applications. , 2020, , .		0
61	Mitigating Insider Threats Using Bio-Inspired Models. Applied Sciences (Switzerland), 2020, 10, 5046.	1.3	9
62	Evolution of cooperation in malicious social networks with differential privacy mechanisms. Neural Computing and Applications, 2023, 35, 12979-12994.	3.2	1
63	A Dynamic DL-Driven Architecture to Combat Sophisticated Android Malware. IEEE Access, 2020, 8, 129600-129612.	2.6	23
64	JSCSP: a Novel Policy-Based XSS Defense Mechanism for Browsers. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	3.7	3
65	Image-Based Feature Representation for Insider Threat Classification. Applied Sciences (Switzerland), 2020, 10, 4945.	1.3	23
66	Privacy-preserving searchable encryption in the intelligent edge computing. Computer Communications, 2020, 164, 31-41.	3.1	13
67	EncodeORE: Reducing Leakage and Preserving Practicality in Order-Revealing Encryption. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1579-1591.	3.7	15
68	Secure and Intelligent Energy Data Management Scheme for Smart IoT Devices. Wireless Communications and Mobile Computing, 2020, 2020, 1-11.	0.8	3
69	Machine learning in cybersecurity: a comprehensive survey. Journal of Defense Modeling and Simulation, 2022, 19, 57-106.	1.2	55
70	Tracking the Insider Attacker: A Blockchain Traceability System for Insider Threats. Sensors, 2020, 20, 5297.	2.1	8
71	Trustworthy blockchainâ€based medical Internet of thing for minimal invasive surgery training simulator. Concurrency Computation Practice and Experience, 2022, 34, e5816.	1.4	2
72	A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. Applied Sciences (Switzerland), 2020, 10, 5208.	1.3	39

#	Article	IF	Citations
73	Insider Attack Detection for Science DMZs Using System Performance Data. , 2020, , .		0
74	Cyber Resilience in Healthcare Digital Twin on Lung Cancer. IEEE Access, 2020, 8, 201900-201913.	2.6	55
75	A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access, 2020, 8, 209802-209834.	2.6	50
76	Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey. IEEE Access, 2020, 8, 197158-197172.	2.6	32
77	A Hybrid Key Agreement Scheme for Smart Homes Using the Merkle Puzzle. IEEE Internet of Things Journal, 2020, 7, 1061-1071.	5.5	12
78	DDoS Attacks Detection with AutoEncoder. , 2020, , .		32
79	Empirical Detection Techniques of Insider Threat Incidents. IEEE Access, 2020, 8, 78385-78402.	2.6	19
80	CD-VulD: Cross-Domain Vulnerability Discovery Based on Deep Domain Adaptation. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 438-451.	3.7	28
81	Software Vulnerability Detection Using Deep Neural Networks: A Survey. Proceedings of the IEEE, 2020, 108, 1825-1848.	16.4	214
82	SDCCP: Control the network using softwareâ€defined networking and endâ€toâ€end congestion control. Concurrency Computation Practice and Experience, 2020, , e5716.	1.4	0
83	Code analysis for intelligent cyber systems: A data-driven approach. Information Sciences, 2020, 524, 46-58.	4.0	25
84	Fully Homomorphic based Privacy-Preserving Distributed Expectation Maximization on Cloud. IEEE Transactions on Parallel and Distributed Systems, 2020, 31, 2668-2681.	4.0	7
85	A dynamic and verifiable multi-keyword ranked search scheme in the P2P networking environment. Peer-to-Peer Networking and Applications, 2020, 13, 2342-2355.	2.6	11
86	From Coarse to Fine (FC2F): A New Scheme of Colorizing Thermal Infrared Images. IEEE Access, 2020, 8, 111159-111171.	2.6	6
87	Detection of Social Network Spam Based on Improved Extreme Learning Machine. IEEE Access, 2020, 8, 112003-112014.	2.6	29
88	Privacy-preserving federated k-means for proactive caching in next generation cellular networks. Information Sciences, 2020, 521, 14-31.	4.0	33
89	Frame-by-frame Wi-Fi attack detection algorithm with scalable and modular machine-learning design. Applied Soft Computing Journal, 2020, 91, 106188.	4.1	5
90	Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning. IEEE Transactions on Network and Service Management, 2020, 17, 30-44.	3.2	75

#	Article	IF	Citations
91	Secure and Efficient Data Sharing in Dynamic Vehicular Networks. IEEE Internet of Things Journal, 2020, 7, 8208-8217.	5.5	13
92	Obfuscation of Malicious Behaviors for Thwarting Masquerade Detection Systems Based on Locality Features. Sensors, 2020, 20, 2084.	2.1	10
93	Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. Journal of Network and Computer Applications, 2020, 161, 102631.	5.8	73
94	Exploring anomalous behaviour detection and classification for insider threat identification. International Journal of Network Management, 2021, 31, e2109.	1.4	18
95	Against Insider Threats with Hybrid Anomaly Detection with Local-Feature Autoencoder and Global Statistics (LAGS). IEICE Transactions on Information and Systems, 2020, E103.D, 888-891.	0.4	4
96	Fooling intrusion detection systems using adversarially autoencoder. Digital Communications and Networks, 2021, 7, 453-460.	2.7	20
97	Battling against cyberattacks: towards pre-standardization of countermeasures. Cluster Computing, 2021, 24, 57-81.	3.5	11
99	Threat Analysis using N-median Outlier Detection Method with Deviation Score. International Journal of Advanced Computer Science and Applications, 2021, 12, .	0.5	1
100	The Efficiency of Vulnerability Detection Based on Deep Learning. Advances in Intelligent Systems and Computing, 2021, , 449-455.	0.5	0
101	Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. IEEE/CAA Journal of Automatica Sinica, 2022, 9, 377-391.	8.5	150
103	Encrypted Data Retrieval and Sharing Scheme in Spaceâ€"Airâ€"Ground-Integrated Vehicular Networks. IEEE Internet of Things Journal, 2022, 9, 5957-5970.	5.5	5
104	A Survey of Android Malware Detection with Deep Neural Models. ACM Computing Surveys, 2021, 53, 1-36.	16.1	156
105	An ultra light weight and secure RFID batch authentication scheme for IoMT. Computer Communications, 2021, 167, 48-54.	3.1	20
106	Detecting Pronunciation Errors in Spoken English Tests Based on Multifeature Fusion Algorithm. Complexity, 2021, 2021, 1-11.	0.9	2
107	Emotion Monitoring for Preschool Children Based on Face Recognition and Emotion Recognition Algorithms. Complexity, 2021, 2021, 1-12.	0.9	10
108	Effective Dealing with Insider Threats a Comparison of Qualitative and Quantitative Research. Asian Journal of Research in Computer Science, 0, , 22-28.	0.0	0
109	A Multi-Tiered Framework for Insider Threat Prevention. Electronics (Switzerland), 2021, 10, 1005.	1.8	12
110	Using Dirichlet Marked Hawkes Processes for Insider Threat Detection. Digital Threats Research and Practice, 2022, 3, 1-19.	1.7	1

#	Article	IF	Citations
111	Secure Collaborative Deep Learning Against GAN Attacks in the Internet of Things. IEEE Internet of Things Journal, 2021, 8, 5839-5849.	5.5	16
112	Static Analysis of Source Code Vulnerability Using Machine Learning Techniques: A Survey. , 2021, , .		2
113	Training regime influences to semi-supervised learning for insider threat detection. , 2021, , .		4
114	Deep learning for insider threat detection: Review, challenges and opportunities. Computers and Security, 2021, 104, 102221.	4.0	86
115	Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems. Journal of Information Security and Applications, 2021, 58, 102717.	1.8	49
116	Insider Threat Detection Using An Unsupervised Learning Method: COPOD. , 2021, , .		4
117	Matching Subsequence Music Retrieval in a Software Integration Environment. Complexity, 2021, 2021, 1-12.	0.9	2
118	Deep neural-based vulnerability discovery demystified: data, model and performance. Neural Computing and Applications, 2021, 33, 13287-13300.	3.2	12
119	Trustworthy Image Fusion with Deep Learning for Wireless Applications. Wireless Communications and Mobile Computing, 2021, 2021, 1-9.	0.8	2
120	LDuAP: lightweight dual auditing protocol to verify data integrity in cloud storage servers. Journal of Ambient Intelligence and Humanized Computing, 2022, 13, 3787-3805.	3.3	7
121	Machine Learning for Detecting Data Exfiltration. ACM Computing Surveys, 2022, 54, 1-47.	16.1	21
122	PMAB: A Public Mutual Audit Blockchain for Outsourced Data in Cloud Storage. Security and Communication Networks, 2021, 2021, 1-11.	1.0	3
123	Anomaly Detection for Insider Threats Using Unsupervised Ensembles. IEEE Transactions on Network and Service Management, 2021, 18, 1152-1164.	3.2	42
124	Insider Threat Detection using Deep Autoencoder and Variational Autoencoder Neural Networks. , 2021, , .		9
125	Survival analysis for insider threat. Computational and Mathematical Organization Theory, 2022, 28, 335-351.	1.5	4
126	Deep learning algorithms for cyber security applications: A survey. Journal of Computer Security, 2021, 29, 447-471.	0.5	9
127	Identification of Unintentional Perpetrator Attack Vectors using Simulation Game: A Case Study. , 0, , .		1
128	Image-Based Insider Threat Detection via Geometric Transformation. Security and Communication Networks, 2021, 2021, 1-18.	1.0	4

#	Article	IF	Citations
129	Insider attack mitigation in a smart metering infrastructure using reputation score and blockchain technology. International Journal of Information Security, 2022, 21, 527-546.	2.3	9
130	An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques. Entropy, 2021, 23, 1258.	1.1	53
131	Establishing forensics capabilities in the presence of superuser insider threats. Forensic Science International: Digital Investigation, 2021, 38, 301263.	1.2	1
132	Intelligent Intraoperative Haptic-AR Navigation for COVID-19 Lung Biopsy Using Deep Hybrid Model. IEEE Transactions on Industrial Informatics, 2021, 17, 6519-6527.	7.2	11
133	Kalman prediction-based virtual network experimental platform for smart living. Computer Communications, 2021, 177, 156-165.	3.1	1
134	DIGFuPAS: Deceive IDS with GAN and function-preserving on adversarial samples in SDN-enabled networks. Computers and Security, 2021, 109, 102367.	4.0	21
135	Secure Distributed Mobile Volunteer Computing with Android. ACM Transactions on Internet Technology, 2022, 22, 1-21.	3.0	8
136	Machine Learningâ€“based Cyber Attacks Targeting on Controlled Information. ACM Computing Surveys, 2022, 54, 1-36.	16.1	59
137	Social Characteristic-Based Propagation-Efficient PBFT Protocol to Broadcast in Unstructured Overlay Networks. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3621-3639.	3.7	3
138	Deep Belief Network-Based Multifeature Fusion Music Classification Algorithm and Simulation. Complexity, 2021, 2021, 1-10.	0.9	10
139	Data-Driven Android Malware Intelligence: A Survey. Lecture Notes in Computer Science, 2019, , 183-202.	1.0	14
140	Unsupervised Insider Detection Through Neural Feature Learning and Model Optimisation. Lecture Notes in Computer Science, 2019, , 18-36.	1.0	5
141	Data Augmentation for Insider Threat Detection with GAN. , 2020, , .		16
142	Lightweight and Certificateless Multi-Receiver Secure Data Transmission Protocol for Wireless Body Area Networks. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1464-1475.	3.7	21
143	A Survey of IoT Applications in Blockchain Systems. ACM Computing Surveys, 2021, 53, 1-32.	16.1	198
144	A NEW TAXONOMY OF INSIDER THREATS; AN INITIAL STEP IN UNDERSTANDING AUTHORIZED ATTACK. International Journal of Information Systems and Management, 2018, 1, 1.	0.2	2
145	Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics (Switzerland), 2020, 9, 1460.	1.8	30
146	Cyber-Security and Its Future Challenges. International Journal of Information Security and Cybercrime, 2021, 10, 38-50.	0.3	0

#	Article	IF	Citations
147	A Visualization-Based Analysis on Classifying Android Malware. Lecture Notes in Computer Science, 2019, , 304-319.	1.0	1
148	Simulation Games Platform for Unintentional Perpetrator Attack Vector Identification. , 2020, , .		3
150	Emotions Behind Drive-by Download Propagation on Twitter. ACM Transactions on the Web, 2020, 14, 1-26.	2.0	4
151	Pseudo stereo output synthesis of wind instruments based on computer multimedia technology. , 2020, , .		0
152	Doc2vec-Based Insider Threat Detection through Behaviour Analysis of Multi-source Security Logs. , 2020, , .		4
153	Temporal Behavior in Network Traffic as a Basis for Insider Threat Detection. , 2020, , .		0
154	Domain adaptation for Windows advanced persistent threat detection. Computers and Security, 2022, 112, 102496.	4.0	12
155	Performing Attack Halting Process with Digital Pattern and Proactive Model Resolving the Security Issues in IoT Based Models. Pattern Recognition Letters, 2021, 152, 428-435.	2.6	1
156	Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation. Forensic Science International: Digital Investigation, 2021, 38, 301126.	1.2	8
157	Detecting Insider Threat from Behavioral Logs Based on Ensemble and Self-Supervised Learning. Security and Communication Networks, 2021, 2021, 1-11.	1.0	7
158	A Context-Aware Neural Embedding for Function-Level Vulnerability Detection. Algorithms, 2021, 14, 335.	1.2	8
159	Image Speckle Denoising for Securing Internet of Smart Sensors. Security and Communication Networks, 2021, 2021, 1-10.	1.0	1
160	Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions. IEEE Communications Surveys and Tutorials, 2022, 24, 160-209.	24.8	66
161	Channel-State-Based Fingerprinting Against Physical Access Attack in Industrial Field Bus Network. IEEE Internet of Things Journal, 2022, 9, 9557-9573.	5.5	7
162	Process mining usage in cybersecurity and software reliability analysis: A systematic literature review. Array, 2022, 13, 100120.	2.5	5
163	A Novel Perspective to Threat Modelling using Design Thinking and Agile Principles. , 2020, , .		7
164	GSketch: A Comprehensive Graph Analytic Approach for Masquerader Detection Based on File Access Graph. , 2021, , .		2
165	Developing Visualisations to Enhance an Insider Threat Product: A Case Study. , 2021, , .		3

#	Article	IF	Citations
166	Digital Twin forÂCybersecurity: Towards Enhancing Cyber Resilience. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2022, , 57-76.	0.2	5
167	Deep Neural Embedding for Software Vulnerability Discovery: Comparison and Optimization. Security and Communication Networks, 2022, 2022, 1-12.	1.0	13
168	Cybersecurity Analysis via Process Mining: A Systematic Literature Review. Lecture Notes in Computer Science, 2022, , 393-407.	1.0	3
169	Detecting insider threat within institutions using CERT dataset and different ML techniques. Periodicals of Engineering and Natural Sciences, 2021, 9, 873.	0.3	4
170	SDGen: A Scalable, Reproducible and Flexible Approach to Generate Real World Cyber Security Datasets. Communications in Computer and Information Science, 2022, , 102-115.	0.4	3
172	Cyber Information Retrieval Through Pragmatics Understanding and Visualization. IEEE Transactions on Dependable and Secure Computing, 2023, 20, 1186-1199.	3.7	1
173	Intelligent detection of vulnerable functions in software through neural embeddingâ€based code analysis. International Journal of Network Management, 2023, 33, .	1.4	4
174	Techniques and countermeasures for preventing insider threats. PeerJ Computer Science, 2022, 8, e938.	2.7	4
175	Character-level word encoding deep learning model for combating cyber threats in phishing URL detection. Computers and Electrical Engineering, 2022, 100, 107868.	3.0	12
176	Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. Connection Science, 2022, 34, 895-910.	1.8	18
177	NGS: Mitigating DDoS Attacks using SDN-based Network Gate Shield. , 2021, , .		4
178	Towards Countering the Insider Reconnaissance Using a Combination of Shuffling and Diversity Moving Target Defense Techniques. Engineering, Technology & Applied Science Research, 2021, 11, 7745-7749.	0.8	0
179	A Taxonomy for Threat Actorsâ€™ Delivery Techniques. Applied Sciences (Switzerland), 2022, 12, 3929.	1.3	3
180	Cyber Code Intelligence for Android Malware Detection. IEEE Transactions on Cybernetics, 2023, 53, 617-627.	6.2	12
181	Social Networking Security during COVID-19: A Systematic Literature Review. Wireless Communications and Mobile Computing, 2022, 2022, 1-21.	0.8	3
182	Memory-Augmented Insider Threat Detection with Temporal-Spatial Fusion. Security and Communication Networks, 2022, 2022, 1-19.	1.0	2
183	A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica, 2022, 9, 784-800.	8.5	116
184	Digital-Twin-Enabled IoMT System for Surgical Simulation Using rAC-GAN. IEEE Internet of Things Journal, 2022, 9, 20918-20931.	5.5	14

#	Article	IF	Citations
185	An Insider Threat Detection Model Using One-Hot Encoding and Near-MissÂUnder-Sampling Techniques. Algorithms for Intelligent Systems, 2022, , 183-196.	0.5	1
186	Compliance Checking Based Detection of Insider Threat in Industrial Control System of Power Utilities. , 2022, , .		4
187	Insider Attack Detection and Prevention using Server Authentication using Elgamal Encryption. , 2022, , .		1
188	Role-based lateral movement detection with unsupervised learning. Intelligent Systems With Applications, 2022, 16, 200106.	1.9	6
189	Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. Information (Switzerland), 2022, 13, 404.	1.7	4
190	Distributed PEPâ€"PDP Architecture for Cloud Databases. Wireless Personal Communications, 0, , .	1.8	0
191	Identifying Incentives forÂExtortion inÂProof ofÂStake Consensus Protocols. Lecture Notes in Networks and Systems, 2023, , 109-118.	0.5	0
192	Evaluating Membership Inference Through Adversarial Robustness. Computer Journal, 2022, 65, 2969-2978.	1.5	4
193	Optimal weighted fusion based insider data leakage detection and classification model for Ubiquitous computing systems. Sustainable Energy Technologies and Assessments, 2022, 54, 102815.	1.7	3
194	A review for insider threats detection using machine learning. AIP Conference Proceedings, 2022, , .	0.3	1
195	Space-Efficient Storage Structure of Blockchain Transactions Supporting Secure Verification. IEEE Transactions on Cloud Computing, 2022, , 1-15.	3.1	0
196	An Effective Insider Threat Detection Apporoach Based onÂBPNN. Lecture Notes in Computer Science, 2022, , 231-243.	1.0	0
197	Robust Anomaly-Based Insider Threat Detection Using Graph Neural Network. IEEE Transactions on Network and Service Management, 2023, 20, 3717-3733.	3.2	0
198	The application of neural network for software vulnerability detection: a review. Neural Computing and Applications, 2023, 35, 1279-1301.	3.2	2
199	Random resampling algorithms for addressing the imbalanced dataset classes in insider threat detection. International Journal of Information Security, 2023, 22, 611-629.	2.3	2
200	Enhancing false negative and positive rates for efficient insider threat detection. Computers and Security, 2023, 126, 103066.	4.0	5
202	Implementing Data Exfiltration Defense in Situ: A Survey of Countermeasures and Human Involvement. ACM Computing Surveys, 2023, 55, 1-37.	16.1	3
203	CapsITD: Malicious Insider Threat Detection Based onÂCapsule Neural Network. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2023, , 57-71.	0.2	0

#	Article	IF	Citations
204	Digital twins and cybersecurity in healthcare systems. , 2023, , 195-221.		0
205	An Analysis of Insider Attack Detection Using Machine Learning Algorithms. , 2022, , .		0
206	Detecting vulnerabilities in IoT software: New hybrid model and comprehensive data analysis. Journal of Information Security and Applications, 2023, 74, 103467.	1.8	1
207	Temporal feature aggregation with attention for insider threat detection from activity logs. Expert Systems With Applications, 2023, 224, 119925.	4.4	5
208	Addressing insider attacks via forensic-ready risk management. Journal of Information Security and Applications, 2023, 73, 103433.	1.8	4
209	Study ofÂanÂApproach Based onÂtheÂAnalysis ofÂComputer Program Execution Traces forÂthe Detection ofÂVulnerabilities. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2022, , 105-115.	0.2	0
210	A High Accuracy and Adaptive Anomaly Detection Model With Dual-Domain Graph Convolutional Network for Insider Threat Detection. IEEE Transactions on Information Forensics and Security, 2023, 18, 1638-1652.	4.5	2
211	User Behaviour based Insider Threat Detection using a Hybrid Learning Approach. Journal of Ambient Intelligence and Humanized Computing, 2023, 14, 4573-4593.	3.3	4
212	Personalized User Profiles-based Insider Threat Detection for Distributed File System. , 2022, , .		0
213	Constructing a Network Graph of File Tracking Results Against Information Leakage. , 2022, , .		1
214	Research Opportunity of Insider Threat Detection based on Machine Learning Methods. , 2023, , .		0
215	Multi-source data fusion for insider threat detection using residual networks. , 2022, , .		1
218	Intelligent Intrusion Detection Algorithm Based on Multi-Attack for Edge-Assisted Internet of Things. Advances in Information Security, 2023, , 119-135.	0.9	5
219	CAS - Attention based ISO/IEC 15408â€"2 Compliant Continuous Audit System for Insider Threat Detection. , 2023, , .		0
224	Cyber Security Culture as a Resilience-Promoting Factor for Human-Centered Machine Learning and Zero-Defect Manufacturing Environments. Lecture Notes in Mechanical Engineering, 2024, , 741-752.	0.3	1
225	UAG: User Action Graph Based on System Logs for Insider Threat Detection. , 2023, , .		0
227	A Teacher-Student Knowledge Distillation Framework for Enhanced Detection of Anomalous User Activity. , 2023, , .		0
229	Insider Threat Classification Using KNN Machine-Learning Technique. , 2023, , .		0

#	Article	IF	Citations
230	Insider Threat Detection: Using Classification Models. , 2023, , .		0
231	Detection of Insider Threats Using Deep Learning. , 2023, , .		0
238	Data Leakage Detection Using ML. , 2023, , .		0
240	AI-Driven Cyber Risk Management Framework. Lecture Notes in Networks and Systems, 2024, , 571-584.	0.5	0
241	Hierarchical Classification Using Ensemble of Feed-Forward Networks for Insider Threat Detection from Activity Logs. , 2023, , .		0